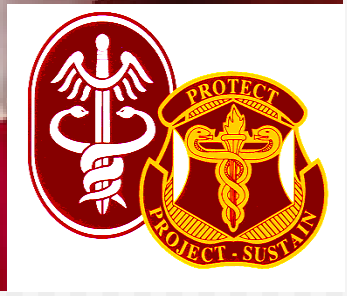
# Operations Security



# Why OPSEC?

- **U.S. Defense Industry targeted by 100+ nations**
- **Industry lost $1.6 trillion to competitors in 2002**
- **2004:  Over $19 Billion on security**
- ***85% of large companies & federal agencies have detected security breaches**
- ***80% of corporate security breaches originate internally**

# The Threat is Growing

" **The number of known adversaries conducting research on information attacks is increasing rapidly and includes intelligence services, criminals, industrial competitors, hackers, and aggrieved or disloyal insiders".**

* Excerpt from speech by Mr. George Tenet, Director, CIA, delivered at the Georgia Institute of Technology, Atlanta, Georgia.

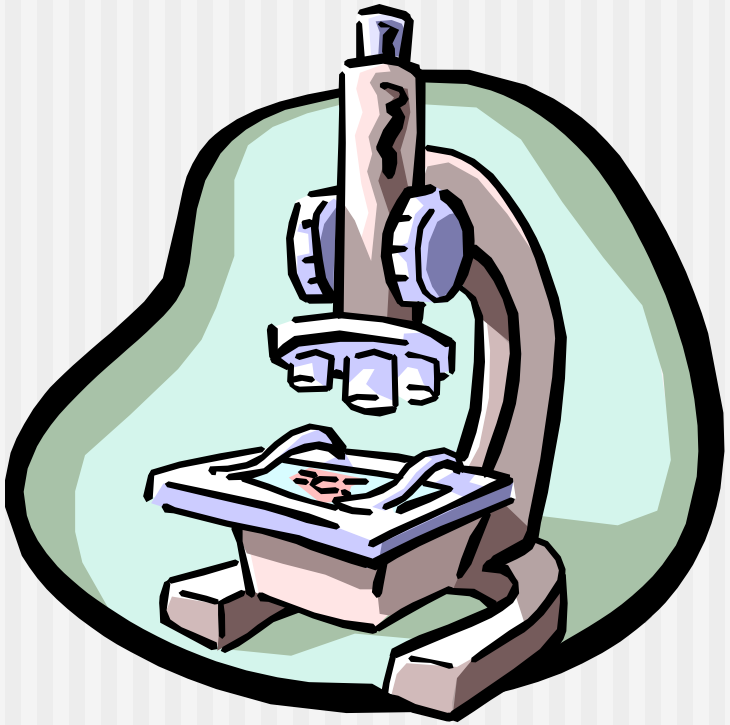
# Cyber Attacks

- **“The number of cyber attacks has increased and the focus has changed from “unstructured” probes by teen hackers to “structured” attacks by more advanced and better organized adversaries.”**
- **Structured attacks are so sophisticated that “we don’t know to what degree” the United States is being attacked.**

- Remarks by Lt. General Kenneth Minihan, Director, National Security Agency, in testimony to the U.S. Congress on Cyber Warfare as reported by Federal Computer Week magazine, June 15, 1998.

# OPSEC

- ***Analytical Process***
- ***Generally Unclassified Information***
- ***<u>Adversary Perspective</u>***



# Five Steps

CRITICAL INFORMATION

VULNERABILITY

THREAT

RISK ANALYSIS

COUNTERMEASURE

# Assess the Threat

- **Who Is The Adversary?**
  - **FOREIGN GOVERNMENTS**
    **COMPETETORS**
    **TERRORISTS**
    **CRIMINALS**
    **HACKERS**
  - **DISGRUNTLED EMPLOYEES**
  - **DISHONEST EMPLOYEES**

# Methods of Collection

- Headhunters
- Foreign Visits
- Unsolicited Requests
- Joint Ventures / Research
- Internet
- Surveillance / Entry
- Exhibits / Conventions
- Co-opting Present / Former Employees

# Trash-INT

- **Social Security Numbers**
- **Addresses & Phone Numbers**
- **Call Signs**
- **Code Names**
- **Tech Manuals**
- **Phone Messages**
- **PIN Numbers**

# Trash-INT (cont'd)

- Leave Application
- Travel Orders
- Floor Plans
- Phone Bills
- Shipping Receipts
- Purchase Orders
- Contracts

# Critical Information

- **Information pointing to your intent, capabilities, vulnerabilities, or strengths.**
- **Information an adversary needs**
- **Pieces of the puzzle**

# Vulnerability

- **Visible or known weaknesses an adversary can exploit to obtain critical information.**
- **Most Common:**
  - **Inappropriate use of email / attachments / web**
  - **Lack of awareness: don't know what to protect, or who to protect it from**
  - **Poor access controls**
  - **Failure to practice need to know**
  - **Failure to comply with security policies**

# Indicator

- **Any Observable or Detectable Activities**

**Or**

- **A piece of Information Pointing to Critical Information**

# Indicators in Context

- **American Rifleman Magazine**
- **Police Chief Magazine**
- **British Heritage Magazine**
- **Saint Andrews Society of Maryland**
- **Tischer Range Rover Inc.**
- **Prince George's County Pensions & Benefits**
- **1st UNION MORTGAGE COMPANY**
- **University of Maryland Alumni Assn.**
- **FBI National Academy Associates**
- **Frederick County National Bank**
- **Dean Whitter Reynolds Inc.**
- **Frederick Chapter, Royal Scottish Country Dance Society**

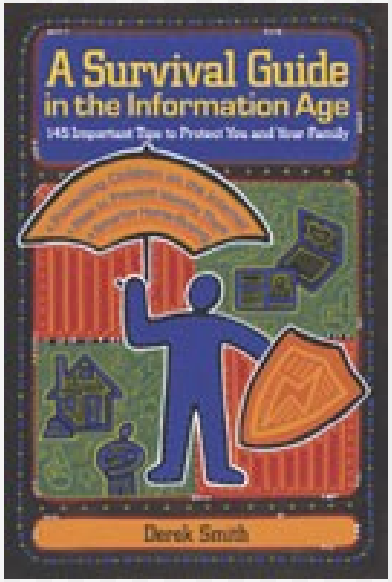
# Impact

- **Cost of the adversary's success**
- **If the adversary exploits your vulnerability, what will it cost you?**
  - **Money**
  - **People**
  - **Time**
  - **Efficiency**
  - **Effectiveness**
  - **Reputation**

# Risk

- **The likelihood of an Undesirable Event Occurring and the Consequences of that Occurrence!**

- **Combination of Threat, Vulnerability and Impact**



# Countermeasure

- Anything That Works!
- Cost Benefit Analysis

# Summary

- OPSEC is an Analytic Process
- OPSEC is Adversary-Oriented
- Every Operation Has Vulnerabilities
- All Indicators Cannot Be Eliminated
- Risk Can Be Mitigated (vs Avoided)
- An Effective Countermeasure is a Good Countermeasure (anything that works)

# For More Information -

- Your OPSEC Officer can be reached at,

301-619-7281/DSN 343

Program Manager 301-619-3334/DSN 343

The Interagency OPSEC Support (IOSS) has OPSEC products and services which are available to government agencies and their contractors. The IOSS can be reached via their website (www.ioss.gov) or by phone (443-479-4677).